

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

09/08/2020

SUBJECT:

Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Android OS builds utilizing Security Patch Levels issued prior to September 5, 2020.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for remote code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could allow for Escalation of Privileges (CVE-2020-0074, CVE-2020-0388, CVE-2020-0391, CVE-2020-0401)

- Multiple vulnerabilities in Framework that could allow for Information Disclosure (CVE-2020-0382, CVE-2020-0389, CVE-2020-0390, CVE-2020-0395, CVE-2020-0397, CVE-2020-0399)
- A vulnerability in Media Framework that could allow for Escalation of Privileges (CVE-2020-0392)
- Multiple vulnerabilities in Media Framework that could allow for Information Disclosure (CVE-2020-0245, CVE-2020-0381, CVE-2020-0383, CVE-2020-0384, CVE-2020-0385, CVE-2020-0393)
- Multiple vulnerabilities in System that could allow for Escalation of Privileges (CVE-2020-0386, CVE-2020-0394)
- A vulnerability in System that could allow for Remote Code Execution (CVE-2020-0380)
- Multiple vulnerabilities in System that could allow for Information Disclosure (CVE-2020-0396, CVE-2020-0379)
- Multiple vulnerabilities in Kernel that could allow for Escalation of Privileges (CVE-2020-0402, CVE-2020-0404)
- A vulnerability in Kernel that could allow for Information Disclosure (CVE-2020-0407)
- Multiple vulnerabilities in Google Play system updates that affect Project Mainline components (CVE-2020-0245, CVE-2020-0383)
- Multiple high severity vulnerabilities in MediaTek components that affect the Sound Driver of Android TV, mdla and ATF (CVE-2020-0123, CVE-2020-0229, CVE-2020-0278, CVE-2020-0342)
- Multiple high severity vulnerabilities in Qualcomm Kernel components (CVE-2019-10527, CVE-2019-14117, CVE-2020-3613, CVE-2020-3656, CVE-2020-11124)
- Multiple critical severity vulnerabilities in Qualcomm Closed-source components (CVE-2019-10628, CVE-2019-10629, CVE-2019-13994, CVE-2020-3621, CVE-2020-3634)
- Multiple high severity vulnerabilities in Qualcomm Closed-source components (CVE-2019-10596, CVE-2019-13992, CVE-2019-13995, CVE-2019-14074, CVE-2020-3617, CVE-2020-3620, CVE-2020-3622, CVE-2020-3629, CVE-2020-3671, CVE-2020-11129, CVE-2020-11133, CVE-2020-11135)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of a privileged process. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to only download applications from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

REFERENCES:

Google Android:

<https://source.android.com/security/bulletin/2020-09-01>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10527>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10596>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10628>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10629>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13992>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13994>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13995>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14074>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14117>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0074>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0123>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0229>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0245>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0278>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0342>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0379>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0380>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0381>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0382>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0383>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0384>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0385>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0386>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0388>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0389>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0390>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0391>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0392>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0393>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0394>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0395>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0396>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0397>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0399>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0401>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0402>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0404>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0407>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3613>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3617>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3620>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3621>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3622>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3629>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3634>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3656>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3671>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11124>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11129>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11133>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11135>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>